UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/800,173	03/06/2001	Peter V. Radatti	E-2538	3615

7590 04/10/2007

John F.A. Earley III
86 The Commons at Valley Forge East
1288 Valley Forge Road
P.O.Box 750
Valley Forge, PA 19482-0750

EXAMINER	
YIGDALL, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2192	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/800,173	RADATTI, PETER V.	
	Examiner	Art Unit	
	Michael J. Yigdall	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4,8-15 and 18-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4,8-15 and 18-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to Applicant's submission filed on January 5, 2007. Claims 4, 8-15 and 18-24 are now pending.

Response to Arguments

2. Applicant's arguments with respect to the Heath reference (remarks, pages 9-10) have been fully considered but they are not persuasive.

Applicant contends that one of ordinary skill in the art would not look to combine Heath with the other references (remarks, page 10).

However, Applicant's argument amounts to a mere assertion without a supporting rationale. The Office action mailed on April 13, 2006 set forth a *prima facie* case of obviousness. Pedrizetti discloses an apparatus for transmitting data to a target (see, for example, the abstract). Heath discloses a similar apparatus for transmitting data to a target (see, for example, the abstract). Pedrizetti's apparatus includes a hash (i.e., the "second" hash) that exists on the target (see, for example, column 5, lines 8-11). Pedrizetti does not expressly disclose that the second hash is "installed" on the target. Nonetheless, Heath's apparatus includes a cryptographic digest or hash that is stored at or installed on the target (see, for example, column 5, lines 7-8 and 64-67). As a result, the target is able to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62). One of ordinary skill in the art would have been motivated to enable the target in Pedrizetti to periodically and automatically obtain updates as needed. Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to implement Pedrizetti's apparatus such that the second hash is installed on the target, as Heath suggests.

Applicant further contends that the examiner's application of Heath's "supposed teachings" does not arrive at the present invention (remarks, page 10), and that Heath teaches away from the claimed invention (remarks, page 11).

However, the examiner does not agree with Applicant's characterization of Heath. Applicant states that in the present invention, "the first cryptographic hash is compared to determine whether the download to the target should take place," whereas in Heath, "the application is already downloaded before [the comparison takes] place" (remarks, page 11). However, Heath illustrates in FIG. 4D, for example, comparing the cryptographic hash to determine whether the download should take place (step 419), before downloading the component to the target (step 420).

Moreover, the rejections of the claims are based on a combination of the Pedrizetti, McGuire and Heath references. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981), and *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The teachings of Heath are relied upon only for the suggestion to "install" Pedrizetti's second hash on the target. Pedrizetti and McGuire teach or suggest the other elements recited in the claims.

3. Applicant's arguments with respect to the new claims and the limitations added to the amended claims (remarks, pages 11-13) have been considered but are moot in view of the new

ground(s) of rejection, as set forth below with reference to Ayres and/or further reference to McGuire. Applicant's amendment necessitated the new ground(s) of rejection.

The examiner notes that Applicant's argument with respect to independent claim 21 (remarks, page 12) is not commensurate with the scope of the claim. While Applicant states that dependent claim 20 provides the step of "editing data on said target in order to update data on said target" and that with independent claim 8, as amended, "the editing would be something other than replacing a file" (remarks, page 13), claim 21 is not so limited. Instead, claim 21 recites, broadly, "editing said data on said target in order to update data on said target." There are no further limitations on the step of "editing said data." Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 4 and 8-15 and 18-21 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,151,708 to Pedrizetti et al. (art of record, "Pedrizetti") in view of U.S. Patent No. 6,493,871 to McGuire et al. (art of record, "McGuire") in view of U.S. Patent No. 6,006,034 to Heath et al. (art of record, "Heath").

With respect to claim 4 (currently amended), Pedrizetti discloses an apparatus for transmitting data to a target (see, for example, the abstract) comprising:

(a) a means for updating, present on a distribution media, and further comprising data, data information and a first hash of said data information (see, for example, FIG. 1 and column 1, lines 41-65, which shows a system for updating software from a distribution server, comprising update data, information based on the update, and a hash table based on the information);

(b) a means for transmission between said distribution media and said target (see, for example, pathway 104 in FIG. 1 and column 2, lines 57-61, which shows a means for transmission between the server and client);

(c) a means for obtaining data information from said distribution media (see, for example, column 1, lines 52-56, which shows that update data information is obtained by the client from the distribution server); and

(d) a means for processing said first hash of said data information (see, for example, FIG. 5 and associated text, and column 1, lines 48-59, which shows that the client processes the information to determine the availability of updates);

whereby said means for obtaining data information from said distribution media obtains said first hash from said means for updating present on said distribution media, which first hash is transmitted through said means for transmission to said means for processing, and which upon receipt of said hash of said data information compares said first hash to a second hash installed on said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 48-59, which shows that the hash table and the update data information

is transferred to the client for processing and is compared to a second hash table on the client to determine whether or not the actual update data should be transferred as well).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are cryptographic hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that the first and second hashes are cryptographic hashes and the first hash is comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

McGuire further discloses the limitation wherein said data is less than the content of a file when only portions of a file, and not the entire file itself, require updating, so as to further minimize the amount of data transmitted to the target (see, for example, column 12, lines 26-41).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that said data is less than the content of a file when only portions of a file, and not the entire file itself, require updating, such as taught by McGuire, so as to further minimize the amount of data transmitted to the target.

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-8) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

With respect to claim 8 (currently amended), Pedrizetti discloses a computer-implemented method for transmitting data to a target (see, for example, the abstract) comprising the steps of:

(a) transmitting a first hash of data information from a first distribution media to said target (see, for example, column 1, lines 45-49, which shows that a hash table based on the update data information is transferred to the client from the distribution server);

(b) comparing said first hash to a second hash installed on said target in order to determine if data information should be transmitted to said target (see, for example, column 1, lines 49-56, which shows that the hash table is compared to a second hash table on the client to determine whether or not additional information should be transferred as well);

(c) transmitting said data information from a second distribution media, if necessary, to said target (see, for example, column 1, lines 52-56, which shows that update data information is transferred to the client if needed; also see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a second distribution media, may be used);

(d) comparing said data information with said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 52-59, which shows that the update data information is compared with the client to determine whether or not the actual update data should be transferred as well).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are a cryptographic hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely

identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti such that the hash is a cryptographic hash comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

McGuire further discloses the limitation wherein said data determined to be transmitted to said target is less than the content of a file when only portions of a file, and not the entire file itself, require updating, so as to further minimize the amount of data transmitted to the target (see, for example, column 12, lines 26-41).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that said data determined to be transmitted to said target is less than the content of a file when only portions of a file, and not the entire file itself, require updating, such as taught by McGuire, so as to further minimize the amount of data transmitted to the target.

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-8) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

With respect to claim 9 (previously presented), the rejection of claim 8 is incorporated, and Pedrizetti further discloses obtaining data information from said second distribution media (see, for example, column 1, lines 52-56, which shows that update data information is obtained by the client from the distribution server).

With respect to claim 10 (previously presented), the rejection of claim 9 is incorporated, and Pedrizetti further discloses the limitation wherein obtaining data information from said second distribution media further comprises using an http address to obtain data information (see, for example, column 2, lines 61-65, which shows that an Internet connection may be used

in conjunction with a Web browser for the software update system; also see, for example, FIG. 6A, which shows a Web browser using an HTTP address).

With respect to claim 11 (previously presented), the rejection of claim 8 is incorporated, and Pedrizetti further discloses the limitation wherein the first and second distribution media are the same (see, for example, server 100 in FIG. 1, which shows the software update system using a single server).

With respect to claim 12 (previously presented), the rejection of claim 8 is incorporated, and Pedrizetti further discloses the limitation wherein either the first and second distribution media at least partially comprises a network (see, for example, column 2, lines 57-58, which shows a server in communication with a client over a communications pathway, i.e. in a network).

With respect to claim 13 (previously presented), the rejection of claim 8 is incorporated, and Pedrizetti further discloses preparing said data information from attributes of said data (see, for example, column 5, lines 50-60, which shows an index file having update data information based on attributes of the actual update data, such as version number and package name; note that the step of preparing the index file is inherent to the method).

With respect to claim 14 (previously presented), the rejection of claim 13 is incorporated, and Pedrizetti further discloses the limitation wherein said data comprises one or more software product data files (see, for example, column 1, lines 41-45, which shows that software program updates are transferred from the distribution server to the client).

With respect to claim 15 (previously presented), the rejection of claim 13 is incorporated, and Pedrizetti further discloses preparing said cryptographic hash from said data information (see, for example, column 1, lines 45-48, which shows a hash table prepared from the update data information).

With respect to claim 18 (previously presented), the rejection of claim 8 is incorporated, and Pedrizetti further discloses transmitting said data from a third distribution media to said target (see, for example, column 1, lines 56-59, which shows that update data is transferred to the client from the distribution server; also see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a third distribution media, may be used).

With respect to claim 19 (previously presented), the rejection of claim 18 is incorporated, and Pedrizetti further discloses the limitation wherein the third distribution media at least partially comprises a network (see, for example, column 2, lines 57-58, which shows a server in communication with a client over a communications pathway, i.e. in a network).

With respect to claim 20 (previously presented), the rejection of claim 19 is incorporated, and Pedrizetti further discloses editing data on said target in order to update data on said target (see, for example, column 3, lines 29-41, which shows that data on the client is edited and updated).

With respect to claim 21 (previously presented), Pedrizetti discloses a computer-implemented method for transmitting data to a target (see, for example, the abstract) comprising the steps of:

(a) providing a software product (see, for example, column 1, lines 41-45, which shows that software program updates are provided on a server);

(b) preparing data information about said software product (see, for example, column 5, lines 50-60, which shows an index file having information based on the software update; note that the step of preparing the index file is inherent to the system);

(c) preparing a first hash of data information about said software product (see, for example, column 1, lines 45-48, which shows a hash table prepared from the update data information);

(d) storing said software product on a first distribution media (see, for example, update data 114 in FIG. 1, which shows the software program update data stored on a server);

(e) storing said data information on a second distribution media (see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a second distribution media, may be used for storage);

(f) storing said first hash of data information on a third distribution media (see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a third distribution media, may be used for storage);

(g) transmitting said hash of data information to said target (see, for example, column 1, lines 45-49, which shows that a hash table based on the update data information is transferred to the client);

(h) comparing said first hash to a second hash installed on said target in order to determine if data information should be transmitted to said target (see, for example, column 1,

lines 49-56, which shows that the hash table is compared to a second hash table on the client to determine whether or not additional information should be transferred as well);

(i) transmitting said data information, if necessary, to said target (see, for example, column 1, lines 52-56, which shows that update data information is transferred to the client if needed);

(j) comparing said data information with said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 52-59, which shows that the update data information is compared with the client to determine whether or not the actual update data should be transferred as well);

(k) transmitting said data, if necessary, to said target (see, for example, column 1, lines 56-59, which shows that update data is transferred to the client if needed); and

(l) editing said data on said target in order to update data on said target (see, for example, column 3, lines 29-41, which shows that data on the client is edited and updated).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are a cryptographic hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for

example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti such that the hash is a cryptographic hash comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-8) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

With respect to claim 24 (new), Pedrizetti discloses a computer-implemented method for transmitting data to a target (see, for example, the abstract) comprising the steps of:

(a) providing a software product (see, for example, column 1, lines 41-45, which shows that software program updates are provided on a server);

(b) preparing data information about said software product (see, for example, column 5, lines 50-60, which shows an index file having information based on the software update; note that the step of preparing the index file is inherent to the system);

(c) preparing a first hash of data information about said software product (see, for example, column 1, lines 45-48, which shows a hash table prepared from the update data information);

(d) storing said software product on a first distribution media (see, for example, update data 114 in FIG. 1, which shows the software program update data stored on a server);

(e) storing said data information on a second distribution media (see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a second distribution media, may be used for storage);

(f) storing said first hash of data information on a third distribution media (see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a third distribution media, may be used for storage);

(g) transmitting said hash of data information to said target (see, for example, column 1, lines 45-49, which shows that a hash table based on the update data information is transferred to the client);

(h) comparing said first hash to a second hash installed on said target in order to determine if data information should be transmitted to said target (see, for example, column 1, lines 49-56, which shows that the hash table is compared to a second hash table on the client to determine whether or not additional information should be transferred as well);

(i) transmitting said data information, if necessary, to said target (see, for example, column 1, lines 52-56, which shows that update data information is transferred to the client if needed);

(j) comparing said data information with said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 52-59, which shows that the update data information is compared with the client to determine whether or not the actual update data should be transferred as well);

(k) transmitting said data, if necessary, to said target (see, for example, column 1, lines 56-59, which shows that update data is transferred to the client if needed); and

(l) editing said data on said target in order to update data on said target (see, for example, column 3, lines 29-41, which shows that data on the client is edited and updated).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are a cryptographic hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely

identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti such that the hash is a cryptographic hash comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

McGuire further discloses the limitation wherein said transmitted data comprises one or the other or both of (i) portions of a file and (ii) an editing command to effectuate a change in a file (see, for example, column 12, lines 26-41, which shows that the transmitted data comprises portions of a file in the form of a patch).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that said transmitted data comprises one or the other or both of (i) portions of a file and (ii) an editing command to effectuate a change in a file, such as taught by McGuire, so as to further minimize the amount of data transmitted to the target.

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-8) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

6. Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pedrizetti in view of McGuire in view of U.S. Patent No. 6,389,592 to Ayres et al. (now made of record, "Ayres") in view of Heath.

With respect to claim 22 (new), Pedrizetti discloses an apparatus for transmitting data to a target (see, for example, the abstract) comprising:

(a) a means for updating, present on a distribution media, and further comprising data, data information and a first hash of said data information (see, for example, FIG. 1 and column 1, lines 41-65, which shows a system for updating software from a distribution server,

comprising update data, information based on the update, and a hash table based on the information);

(b) a means for transmission between said distribution media and said target (see, for example, pathway 104 in FIG. 1 and column 2, lines 57-61, which shows a means for transmission between the server and client);

(c) a means for obtaining data information from said distribution media (see, for example, column 1, lines 52-56, which shows that update data information is obtained by the client from the distribution server); and

(d) a means for processing said first hash of said data information (see, for example, FIG. 5 and associated text, and column 1, lines 48-59, which shows that the client processes the information to determine the availability of updates);

whereby said means for obtaining data information from said distribution media obtains said first hash from said means for updating present on said distribution media, which first hash is transmitted through said means for transmission to said means for processing, and which upon receipt of said hash of said data information compares said first hash to a second hash installed on said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 48-59, which shows that the hash table and the update data information is transferred to the client for processing and is compared to a second hash table on the client to determine whether or not the actual update data should be transferred as well).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are cryptographic

hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that the first and second hashes are cryptographic hashes and the first hash is comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

Pedrizetti does not expressly disclose said data transmitted to said target comprising an editing command for editing said target.

However, Ayres teaches a similar apparatus for transmitting data to a target (see, for example, the abstract). Ayres discloses that the data transmitted to the target comprises editing commands for editing the target, so as to reduce the amount to data transmitted to the target (see, for example, column 2, line 55 to column 3, line 4).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti and McGuire such that said data transmitted to said target comprises an editing command for editing said target, such as taught by Ayres, so as to further reduce the amount to data transmitted to the target.

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-8) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti, McGuire and Ayres such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

With respect to claim 23 (new), Pedrizetti discloses an apparatus for transmitting data to a target (see, for example, the abstract) comprising:

(a) a means for updating, present on a distribution media, and further comprising data, data information and a first hash of said data information (see, for example, FIG. 1 and column 1, lines 41-65, which shows a system for updating software from a distribution server,

comprising update data, information based on the update, and a hash table based on the information);

(b) a means for transmission between said distribution media and said target (see, for example, pathway 104 in FIG. 1 and column 2, lines 57-61, which shows a means for transmission between the server and client);

(c) a means for obtaining data information from said distribution media (see, for example, column 1, lines 52-56, which shows that update data information is obtained by the client from the distribution server); and

(d) a means for processing said first hash of said data information (see, for example, FIG. 5 and associated text, and column 1, lines 48-59, which shows that the client processes the information to determine the availability of updates);

whereby said means for obtaining data information from said distribution media obtains said first hash from said means for updating present on said distribution media, which first hash is transmitted through said means for transmission to said means for processing, and which upon receipt of said hash of said data information compares said first hash to a second hash installed on said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 48-59, which shows that the hash table and the update data information is transferred to the client for processing and is compared to a second hash table on the client to determine whether or not the actual update data should be transferred as well).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are cryptographic

hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that the first and second hashes are cryptographic hashes and the first hash is comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

Pedrizetti does not expressly disclose said data transmitted to said target comprising a binary editing command.

However, Ayres teaches a similar apparatus for transmitting data to a target (see, for example, the abstract). Ayres discloses that the data transmitted to the target comprises binary editing commands, so as to reduce the amount to data transmitted to the target (see, for example, column 2, line 55 to column 3, line 4).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti and McGuire such that said data transmitted to said target comprises a binary editing command, such as taught by Ayres, so as to further reduce the amount to data transmitted to the target.

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-8) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti, McGuire and Ayres such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure (see the attached Notice of References Cited).

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Yigdall whose telephone number is (571) 272-3707. The examiner can normally be reached on Monday through Friday from 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Q. Dam can be reached on (571) 272-3695. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MY

Michael J. Yigdall
Examiner
Art Unit 2192

mjy

TUAN DAM
SUPERVISORY PATENT EXAMINER